IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHEN MARIANA ISLANDS

TIANMING WANG, *et al.*, Plaintiff, vs. GOLD MANTIS CONSTRUCTION DECORATION (CNMI), LLC, *et al.*, Defendants.	Case No.: 1:18-cv-00030 AFFIDAVIT OF MICHELE BUSH

I, MICHELE BUSH, hereby declare as follows:

I am a digital forensics expert at Loehrs Forensics, LLC, (formerly Loehrs & Associates, LLC) a firm specializing in digital forensics, located at 1505 North Central Avenue, Suite 111, Phoenix, Arizona 85004. I am competent to testify and the matters contained herein are based on my own personal knowledge.

I hold a Bachelor of Science in Psychology from the University of Arizona and Associate Degrees in Arts and Science from Pima Community College. I have completed extensive forensics training including courses with Guidance Software, Cellebrite, Access Data, and the Information Assurance Certification Review Board. To qualify for forensic training and certifications I was subjected to numerous background checks, assessments, written tests, and practical exams simulating real investigations. As a result of my collective training and testing, I hold vendor-neutral certifications including Certified Computer Examiner (CCE) and Certified Computer Forensics Examiner (CCFE), as well as vendor-specific certifications including

Certified Mobile Forensics Examiner (CMFE), Certified Cellebrite Operator (CCO), Certified Cellebrite Physical Analyst (CCPA), EnCase Certified Examiner (EnCE), and Access Data Certified Examiner (ACE). In addition, I hold a Private Investigator license in the State of Arizona.

I am a member of the International Society of Computer Forensic Examiners (ISCFE), the Scientific Working Group on Digital Evidence (SWGDE), and the Forensic Expert Witness Association (FEWA). ISCFE is an internationally recognized private organization that conducts research and development into emerging technologies and methods in the science of computer forensics. Members are only admitted upon passing the uncompromised Certified Computer Examiner certification process for the competency and ethical standards for forensic computer examiners. SWGDE is a non-profit organization consisting of a maximum of 100 members from law enforcement, academic, and commercial organizations actively engaged in the field of digital forensics to develop cross-disciplinary guidelines and standards for the recovery, preservation, and examination of digital evidence. Members are only admitted in a majority vote by the committee. Lastly, FEWA is a non-profit professional membership organization that verifies its members have testified as an expert witness in at least three cases.

I have conducted hundreds of forensics exams on thousands of electronic evidence items of varying types including mobile devices and testified over 20 times in state and federal court throughout the country. A copy of my Curriculum Vitae is attached as Exhibit A.

I was retained by counsel for third-party witness for the purpose of assisting with matters related to the analysis of electronic evidence in this matter. I have specifically been asked to independently analyze the Apple iPhone XS Max belonging to Lijie Cui and opine on the accuracy of the technical statements included in the declarations of Jonathan Langton. The statements contained in this affidavit are based on, in part: information provided by counsel for third-party witness; discovery including, but not limited to, Declaration of Jonathan Langton dated July 27, 2021, and the Fifth Declaration of Jonathan Langton Concerning Lijie Cui's iCloud Account dated November 24, 2021; my independent analysis of the evidence; and my experience, training and background as a certified forensics examiner.

On January 10, 2022, my office received an Apple iPhone Xs Max bearing serial number F2MXD4M8KPJ4 and two forensic extractions of that phone from Transperfect Legal Solutions ("TLS"). Upon receipt of the evidence, Loehrs Forensics performed a physical inspection of the phone and generated four additional forensic extractions of the phone's memory and SIM card. I found that the iPhone Xs Max is equipped with 64GB of flash memory and a dual nano-SIM tray. The Loehrs Forensics Chain of Custody, evidence photos, and extraction report are attached as Exhibit B.

Mr. Langton opines, in part, from his analysis of the iPhone Xs Max that it was previously backed up to a computer because it contained an iTunes backup password. An iTunes backup password is prompted when an iOS device, such as an iPhone, is connected to a computer that is installed with iTunes and a local backup is completed. By enabling this feature, iTunes will include sensitive information in the backup including account passwords, Health and HomeKit data that a user may want transferred when saving and restoring their phone. Due to the sensitive nature of the material included in that type of backup, iTunes requires encryption and will not backup this user data if a password has not been set. A screenshot of this setting from a sanitized test phone of the same make and model is attached as Exhibit C. In that regard, I agree with Mr. Langton's opinion that for the phone to have an iTunes backup password it must have been previously backed up to a computer.

My independent analysis of the extractions created by TLS revealed evidence that further corroborates the opinion that the phone was backed up to a computer. The iOS records a history of computers used to back up the device within the *iTunesPrefs* file. According to the Advanced Logical extraction created by TLS on June 24, 2021, the *iTunesPrefs* file was last modified on June 22, 2021, and identifies two computers which contain iTunes backups of this device: “MANSUND01” and “SEVENTYTHREE”. The *MANSUND01* computer is the first computer that backed up this phone and likely enabled the iTunes backup password to include system data, software data, user data, and data containing sensitive information. The iOS does not record the date this phone was backed up to the *MANSUND01* computer. The second computer used to backup this device was named *SEVENTYTHREE.* According to TLS’s extraction summary, the forensic station used to acquire this phone in June of 2021 was named *SEVENTYTHREE.* This indicates their computer was recorded as the only other source for an iTunes backup. Furthermore, the forensic extractions created by TLS contain over 26,000 Health records and 400 passwords with activity dating back to December 10, 2018, consistent with data that would only be recovered from a backup if it was encrypted. In that regard, the forensic evidence suggests that the only other iTunes backup for this device exists on the *MANSUND01* computer but is likely encrypted.

Mr. Langton also opines that the unencrypted data extracted by TLS contains a “limited and temporally inconsistent volume of communication data”. It is my opinion that this conclusion is highly subjective because it depends on the configurations, usage, and history of the phone, as well as the method employed to extract data from the phone. For example, iOS offers configuration settings to manage data allocation and storage by automatically deleting text messages over 30 days old. This setting would directly affect the volume of communication data extracted from a phone and, if enabled, I would not expect to find any messages older than 30 days.

Based on my training and experience, a forensic examiner must reset the phone's settings and a perform new backup to circumvent a preexisting iTunes backup password and access the phone's contents. This is corroborated by an Apple support post attached as Exhibit D. Although the specific process used by Mr. Langton was not detailed in the declarations provided for my review, it is likely that the settings were reset during TLS's extraction and any forensic evidence of the phone's prior settings while it was still in possession of Ms. Cui are no longer available or reliable.

Moreover, the extraction method must be considered when opining on the amount of data collected from a device. For iOS devices, a bit-for-bit copy of the device's storage is unavailable to forensic examiners due to physical disk encryption enabled by Apple when manufacturing the devices. This means data residing in unallocated space (i.e. deleted data) is unrecoverable, even to a forensics examiner. The most inclusive iOS extraction method available for the private sector is Cellebrite's Advanced Logical which is limited to allocated data from the file system and installed applications. As such, it is my opinion that no substantive conclusions can be reached regarding the data that any examiner may expect to find on this device.

Mr. Langton further opines that it is "highly likely that Ms. Cui's iPhone Xs Max was 'initialized' on March 21, 2021" based on the presence of that date within the "purplebuddy.plist". The *com.apple.purplebuddy.plist* file is created by the Apple iOS within the *mobile/Library/Preferences* file system directory for the purpose of tracking information about the device including setup, language, county, among other configurations. One *com.apple.purplebuddy.plist* file was extracted from the iPhone Xs Max which defines the

"GuessCountry" key as March 21, 2021, at 03:58:01PM UTC and "SetupLastExit" key as March 22, 2021, at 04:33:30AM UTC. I agree with Mr. Langton's opinions that these keys have been known to update when a device is initialized or reset. However, the *com.apple.purplebuddy.plist* file was created on June 25, 2021, and also defines the "lastPrepareLaunchSentinel" key as June 24, 2021, at 02:26:39PM UTC, while the phone was in the possession of TLS. These additional dates are important to consider when opining on the reliability of the information recorded by this file and what occurred on and around March 21, 2021. For instance, TLS did not report initializing the iPhone Xs Max nor do I have any reason to believe that they did, yet the same file relied upon by Mr. Langton to conclude the phone was initialized in March was also created and written while in TLS's possession. A screenshot of the *com.apple.purplebuddy.plist* file is attached as Exhibit E.

My forensic analysis also revealed that the phone underwent a major iOS update from version 13 to 14 on March 21, 2021. This information was gleaned from the Health application which records a history of the device's iOS version within the *mobile/Library/Health/heatlhdb.sqlite* system file. According to this database, on December 10, 2019, the device was installed with iOS version 12.0. On October 31, 2019, the device was updated to iOS version 13.2. On March 21, 2020, at 07:30:13PM UTC the phone was updated to iOS version 14.4.1. It is plausible that this substantive operating system update caused the dates within the *com.apple.puplebuddy.plist* to update as a form of initialization. A screenshot of the *heatlhdb.sqlite* file is attached as Exhibit F.

Mr. Langton reports that on November 16, 2021, he was able to access the iCloud account registered to the iPhone, but the earliest device backup available was "created after the iPhone had been initialized" and opines that he is "not able to determine when this iCloud account was created" or "whether other iCloud accounts linked to different email addresses may exist".

Despite the limitations imposed by potential settings enabled on the phone and the extraction method used to collect the evidence, data of evidentiary interest regarding the iCloud account history of this device was forensically recovered. Apple iOS stores a history of iCloud accounts accessed by the phone within the *Accounts3.sqlite* system file. My independent analysis of the phone revealed two *Accounts3.sqlite* databases. The first database was created on September 13, 2018, likely during Apple's first initialization of this phone since this make and model was first released to the public on September 21, 2018. The second database was created on December 10, 2018, when the phone was likely first setup by the device owner. According to both databases, the only Apple ID accessed by this phone was *jie133211@gmail.com* beginning on December 10, 2018. Screenshots of these databases and their contents are attached as Exhibit G.

Beyond the *Accounts3.sqlite* database file, forensic searches were conducted throughout all data extracted from the phone using Cellebrite's Physical Analyzer "Watch Lists" and "Advanced Search" features for the string "@qq.com". If this phone was used to login and access a QQ account, I would expect to find references for that account within system and software files maintained by the iOS even if it has since been logged out. This forensic search would identify any instance that a QQ email account was registered or accessed using this device. The forensic searches resulted in five total hits but zero positive matches. That is, the string "@qq.com" resulted in template language within system files referencing the domain that is unrelated to any user's account, and one hit for a contact logged by the WeChat database. Screenshots of these search results are attached as Exhibit H. For those reasons, no forensic evidence was located that this device was installed with the QQ application, used to access a QQ account, or otherwise registered using a QQ email address.

In conclusion, Mr. Langton opines that the phone was initialized on March 21, 2021, and suggests it was restored from a sanitized backup. If the phone was restored from an iTunes backup, I would expect to find a "RestoreInfo" key within the *root/Library/Preferences/com.apple.MobileBackup.plist* system file. The presence of this key would confirm that the phone had been restored from a backup, would specify the date of restoration, and identify the origin of the backup as from iCloud or iTunes. An example of this file from a test Apple iPhone Xs Max is attached as Exhibit I. A review of *root/Library/Preferences/com.apple.MobileBackup.plist* found on the Ms. Cui's Apple iPhone Xs Max revealed it is void of this key. As such, the forensic evidence suggests this phone has not been restored. A screenshot of this *com.apple.MobileBackup.plist* is attached as Exhibit J.

It is also important to note that even if the forensic evidence supported the opinion that the phone had been factory reset on or about March 21, 2021, iTunes does not allow a user to be selective with the data included in a backup. This means a user cannot limit the backup to only photos and call logs and exclude notes, text messages, and emails. Rather, iTunes automates the backup process and will include all data available on that device. Likewise, a user cannot select limited data to restore to a phone from a backup. iTunes will restore all the data within a backup to the phone beyond a user's control.

In summary, it is my opinion the forensic evidence is inconsistent with the device being initialized or factory reset on March 21, 2021, and restored from a backup for the following reasons:

1) System files (e.g., *Accounts3.sqlite*) with original creation dates from 2018 remained intact on the phone, whereas I would expect those dates would be updated to the date a factory reset and restore occurred;

2) The *com.apple.MobileBackup.plist* file was absent key data I would expect to find if a backup had been restored to the phone;

3) The iOS on the device was updated from version 13 to 14 on March 21, 2021, which would highly affect the contents of system files on the devices including the *com.apple.purplebuddy.plist* file.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

DATED January 21, 2022.

MICHELE BUSH